IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Campbell, et. al.	
Serial No.: 10/064,741	Group Art Unit: Not yet assigned
Filed: 8/12/2002	Examiner: Not yet assigned
Title: DIGITAL RIGHTS MANAGEMENT	Attorney Docket No.: I09.001

PETITION TO MAKE SPECIAL (BASED ON PRE-FILING SEARCH) FOR NEW APPLICATION UNDER 37 C.F.R. 1.102(d) AND MPEP §708.02

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Applicants hereby petition to make the above-identified application special. The application has not yet been examined.

1. The Claims

All of the claims presented in the application are believed to be directed to a single invention. However, if the Office should determine that all of the claims presented are not obviously directed to a single invention, Applicants will make an election without traverse as a prerequisite to the grant of special status.

2. Description of Search

A search has been made by a professional searcher (the search firm of Gilman Research Services). The searcher conducted patent searches as follows:

a. USPTO full text searches were conducted in the following class/subclasses:

Class 709 subclass 224;
Class 713 subclasses 201, 210;
Class 714 subclasses 1, 14; and
Class 345 subclass 440.

b. Keyword searches were conducted in the following Lexis-Nexis databases: US Fulltext, European Patents, and Patent Abstracts of Japan.

c. Keyword searches were conducted in the following Dialog databases:

Derwent World Patents (351), WIPO/PCT Patents (349), and INPADOC/Family (345).

d. Keyword searches were conducted in the following non-patent literature services and databases:

Service	Databases
Lexis-Nexis	General News, Industry News, Network World, Communications Daily, Internet Wire, Information Security, LAN Magazine
Dialog	Dissertation Abstracts (35), EconLit (139), Wall Street Journal Abstracts (475), World Reporter (20)
Internet Engines	NorthernLight, Google, All The Web, Open Directory
e-Resources	FedWorld, Software Patent Institute's Database of Software Technologies, Honeynet Project, BlackHat, EETimes, MIT Media Lab, Slashdot, C-net, ZD-net
Usenet Newsgroups	Motley Fool Message Board, Yahoo Message Board, Google Newsgroups (Formerly Deja.com)
Company Sites	Overpeer, Vidius, NetPD, Media Defender, OnSystems, MediaForce, Napster, Gnutella, Morpheus, Kazaa, Grokster, StreamCast Networks, Recourse Technologies
Trade Groups, Associations & Conferences	Recording Industry Association of America, nternational Association for Computer Systems Security

e. Various keywords were used in the keyword searches described above. In particular, the searcher reported using various combinations of the following keywords in his searches:

Decoy	Trojan horse	File sharing	MP3
Files	Defect	Review	Quality
Download	File swapping	Spoofing	Noise
Analyze	Monitor	P2P	Peer to peer
Napster	Gnutella	Morpheus	Kazaa
Grokster	Corrupt	Damage	Bogus
Sabotage	False	Upload	Illegal
Unauthorized	Pirated	Distribution	Reactive
Intercept	Generate	Fictitious content	Populate
Honeypot	Deception server	Façade	Sacrificial lamb
Honeypot zoo	Honeynet	Anti-piracy	Flooding
Spraying			

3. Copies of References

The following references are considered to be the most relevant (as relating to the claimed subject matter) of the references identified by the searcher. All of the references identified by the searcher are cited on the accompanying Information Disclosure Statement. Copies of each of the references are provided with the accompanying Information Disclosure Statement.

a. Patent References

US Patent Serial No. 5,787,068, issued July 28, 1998 to Arps et al.

US Patent Application No. 2002/0069098, published on June 6, 2002

US Patent Application No. 2002/0082999, published on June 27, 2002

US Patent Application No. 2002/0087885, published on July 4, 2002

PCT Application No. WO 01/06373, published on January 25, 2001

PCT Application No. WO 00/70463, published on November 23, 2000

b. Non-patent References

Recourse Technologies: "The Evolution of Deception Technologies as a Means for Network Defense", 11pgs.

Recourse Technologies: "Honeypot Effectiveness Study", by Glogal Integrity Corporation, September 22, 2000, 11pgs.

Jelena Mirkovic, Peter Reiher and Gregory Prier, "A Source Router Approach to DdoS Defense", 16pgs.

Andrew H. Chen and Andrew M. Schroeder, "A Modified Depensation Model for Peer to Peer Networks: Systemic Catastrophes and other Potential Weaknesses", December 17, 2001, Term Paper, 18pgs.

Slashdot, "Spoofing P2P Networks as Marketing Plot", download from http://slashdot.org/article.pl?sid=02/06/10/1852237&mode=thread&tid=141 on 07/10/2002. 22pgs.

MediaForce, Article, download from http://www.mediaforce.com on 07/09/2002. ©2001 All rights reserved. 12pgs.

King, Brad "File Tracker May Go Too Far", May 11, 2001, download from http://www.wired.com/news/print/0,1294,43714,00.html on 07/09/2002. 2pgs. © 1994-2002 Wired Digital Inc. All rights reserve..

Mariano, Gwendolyn "Box office hits pirated over Web", July 10, 2001, download from http://news.com.com/2100-1023-269743.html?legacy=cnet&tag=mn_hd on 07/09/2002. 2pgs. ©1995-2002 CNET Networks, Inc. All rights reserved.

Borland, John "File-trading pressure mounts on ISPs"- Tech News – CNET.com, July 25, 2001, download from http://news.com/2102-1033-270568.html on 07/09/2002.

"SK – PR/News: SK.com Newsletter: Executive Interview [May 2002], download from http://www.sk.com/news/newsletter/current/essay_b.asp on 07/09/2002. 1pg.

Gallivan, Joseph "NAPSTER BOOTLEGGERS IDENTIFIED", 05/03/2000, New York Post, ©2000, N.Y.P. Holdings, Inc. 1pg.

Chmielewski, Dawn C. "Music industry swamps swap networks with phony files", June 27, 2002. Download from http://www.siliconvalley.com/mld/siliconvalley/3560365.htm?template=contentModules/printstory.jsp on 07/09/2002.

Li, Sing - devloperWorks: Java Technology: "Making P2P interoperable: The JXTA story – A hands on, working introduction to the latest P2P technology", August 2001, download from http://www-106.ibm.com/developerworks/java/library/j-p2pint1.html?t=gr,p=Jxta on 08/15/2002. 7pgs.

Edison Media Research, "The National Record Buyers Study II", June 10, 2002, download from http://www.edisonresearch.com/RecordBuyersIIPress.htm on 08/15/2002. © 1998-2002. 3pgs.

Mathews, Anna Wilde and Orwall, Bruce, "Industry to Sue People Abetting Net Song Swaps", Wall Street Journal, July 3, 2002, pg. B1, Col. 5. 2pgs.

Wingfield, Nick, "Behind the Fake Music: Record Industry Plants Decoys To Foil Fans of Free Web Tunes; A Decoy for Sheryl Crow", Wall Street Journal, July 11, 2002, pg. D1, D3, Col. 4

Chmielewski, Dawn C., "Record Labels Open New Fire on Piracy", June 28, 2002, ©2002 KRTBN Knight Ridder Tribune Business News. 2pgs, download from http://www.bayarea.com/mld/bayarea/business3562276.htm on 8/19/2002.

Mathews, Anna Wilde, "The Studios Strike Back – Online Movie Swapping Raises the Ire of Hollywood; Fingering 'Repeat Infringers'", April 26, 2002, The Wall Street Journal, ©2002 Dow Jones & Company, Inc., 2pgs.

"Sabeus Closes C Round Funding Totaling More Than $21 Million", ©2002, Business Wire. 2pgs.

"Vidius Expands Market Presence in Asia; Alvus Announced as Master Distributor for Vidius Japan," ©2002, Business Wire. 2pgs.

TheLAW.com - "Software Coders Work to Trade Music without Using Napster", Knight Ridder/Tribune, October 3, 2000, download from http://64.225.202.40/mediadefender/press%20about%20MD/TheLAW_com.htm on 08/16/2002.

Wheeler, Marilynn, "Dr. Dre to deliver names to Napster", May 9, 2000, ZDNet News, download from http://zdnet.com.com/2102-11-520620.html on 8/16/2002. 2pgs.

Healey, Jon "Pirates Make New Use of Old Technology", 03/01/2002, Los Angeles Times, Home Edition. ©2002 The Times Mirror Company. 2pgs.

Healey, Jon "New Technologies Target Swapping of Bootlegged Files", 02/20/01, Los Angeles Times, Home Edition, ©2001 The Times Mirror Company. 2pgs.

Goodley, Simon "City – Connected – Film pirates face legal clampdown Movie-makers aim to protect copyright, reports...", 01/15/2002, The Daily Telegraph, Telegraph Group Limited, London, 2002. 3pgs.

Flathmann, Jessica "Students Warned About Internet; Officials Say Violating Copyrights Could Bring Suspension, Prosecution;", 11/20/2001, ©2001 The Charlotte Observer. 2pgs.

"Reciprocal And NetPD Forge Strategic Alliance To Foster Digital Commerce and Combat Internet Piracy", 05/30/2001, © 2001 Business Wire. 2pgs.

"City – dotcom telegraph – Studios fear the internet pirates", 06/25/2002, The Daily Telegraph, © Telegraph Group Limited, London, 2002.

Watson, Stephen "Music Cops; The Recording Industry wants to curb downloading music from the internet, so it's asking colleges to police computer use. But music lovers are staying a step ahead", 03/20/2002, ©2002, Buffalo News. 3pgs.

Trefgarne, George "City – 'They're playing our tune' says EMI boss Record head relaxed as internet pirates steal sales, 05/22/2002, The Daily Telegraph, © Telegraph Group Limited, London, 2002. 2pgs.

Edited by Rupert Steiner, "NETPD", 04/14/2002, Sunday Times – London, © Times Newspapers Ltd, 2002. 1pg.

Suzukamo, Leslie Brooks "Internet theft threatens film studios", 05/29/2002, The Star-Ledger Newark, NJ ©2002. 1pg.

Evangelista, Benny "Pirated previews / DivX program makes movie bootlegs easier to distribute – and that has Hollywood worried", 05/10/2001, © 2001 The San Francisco Chronicle. 3pgs.

Myers Jr., George "Teen's site carries on free-music fight", 04/04/2001, The Columbus Dispatch, Home Final, ©2001 Columbus Dispatch. 3pgs.

Healey, John "Company Town Gnutella Targeted for Piracy Control Music: Unlike Napster, the decentralized network cannot be sued by record labels. The RIAA is seeking detection technology", 03/29/2001, Los Angeles Times, Home Edition, © 2001 The Times Mirror Company. 2pgs.

Healey, Jon "File-Sharing Firms Feud Over Users Internet: Kazaa.com recruits from Morpheus' network after glitch prevents some from using the service", 03/02/2002, Los Angeles Times, Home Edition, ©2002 The Times Mirror Company. 2pgs.

Suzukamo, Leslie Brooks "Movie types try to scuttle or find a way to control the downloading craze", 06/11/2002, ©2002, The Kansas City Star. 2pgs.

4. Detailed Discussion of the References

A detailed discussion of the references identified by the searcher, identifying how the claimed subject matter is distinguished, is attached hereto.

5. Fee

The fee of $130.00 required by 37 CFR 1.17(h) is to be paid by the attached credit card authorization. Although no additional fees are believed due, the PTO is hereby authorized to charge any fees due in connection with this application to Deposit Account Number 50-1852.

In view of the above, Applicants request that the Petition to Make Special be granted and the examination of the application be advanced.

Respectfully Submitted,

August 23, 2002
Date

Kurt M. Maschoff
Attorney for Applicants
Reg. No. 38,235

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Campbell, et. al.	Group Art Unit: Not yet assigned
Serial No.: 10/064,741	Examiner: Not yet assigned
Filed: 8/12/2002	Attorney Docket No.: I09.001
Title: DIGITAL RIGHTS MANAGEMENT	

DETAILED DISCUSSION OF THE CLAIMS RELATIVE TO THE ART IN SUPPORT OF PETITION TO MAKE SPECIAL

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

In support of the attached Petition to Make Special (filed herewith), Applicants submit the following remarks.

Discussion of the Claimed Invention

Embodiments of the present invention relate to network techniques for addressing the unauthorized distribution of digital content such as movies, songs, etc. Unauthorized distribution of such content is increasing as a result of the use of file sharing networks such as Gnutella, etc. Content owners would like to reduce the unauthorized copying. Embodiments of the present invention operate to reduce unauthorized copying by disseminating decoy files throughout file sharing networks. These decoys each have one or more defects. Embodiments of the present invention provide an ability to intelligently create, disseminate, monitor, and analyze the distribution of these decoys.

In some embodiments, an item of content is protected by monitoring a plurality of file sharing networks to identify at least a first file sharing network having the item of content. At least first and second reference files associated with the item of content are created, where the first and second reference files each have a different format. A plurality of decoy files are created, including a first set of decoy files created from the first reference file, and a second set of decoy files created from the second reference file, where each of the decoy files includes a defect. The decoy files are disseminated to the first file sharing network. The effects of the dissemination may then be monitored to determine if any adjustments should be made (e.g., such as a further dissemination or a modification of the dissemination characteristics, etc.).

Independent claim 1, for example, recites a method for protecting an item of content which includes monitoring a plurality of file sharing networks to identify at least one network having the item of content; creating at least first and second references files associated with the

item of content, where the first and second reference files each have a different format; creating a plurality of decoy files, including a first set created from the first reference file and a second set created from the second reference file, each of the decoys having a defect; and disseminating the decoys to the file sharing network.

Discussion of Cited References

As noted in the attached Petition to Make Special, Applicants have conducted a pre-filing search. The search uncovered a number of references, some of which are believed to deserve individual discussion; others are collectively discussed as "Other Background Art" below. Other references not specifically discussed are believed to contain cumulative material. The following are presented in no particular order.

(1) US Patent Application No. 2002/0069098, published on June 6, 2002, and filed by Schmidt (the "Schmidt reference").

The Schmidt reference describes a system and method for protecting proprietary material on computer networks. In general, the Schmidt reference describes a system for searching and finding privately owned content and private information and then storing the results for analysis so that a number of "cease and desist" letters can be sent out to individuals who are providing or retrieving unauthorized copys of copyrighted content.

The system first identifies copys of content on file sharing networks. When a copy is found, the content is downloaded and a routine is run to identify the content. If no tag for the content exists, the content is manually verified to determine if it has a copyright and should be protected. If it should be protected, information is stored in a database. If the content should be protected, it is protected by "logging, stopping, or replacing the content during its transfer." (see paragraph [0032]). In particular, the Schmidt reference details a "cease and desist notification process" for use in protecting content once unauthorized copying is detected. This process is described at, for example, paragraphs [0049]-[0061].

The Schmidt reference fails to teach or suggest a system as claimed in independent claims 1 and 31 of the present invention where at least first and second reference files are created (in different formats) for each item of content to be protected. Nor does Schmidt describe a method where at least two sets of decoy files are created, each having defects, and each created from the different reference files. In this manner, embodiments of the present invention permit the creation and dissemination of a number of different types of decoys which mimic the type and format of files which are being copied on the file sharing networks. There is simply no suggestion in the Schmidt reference to prevent copying by using such decoys or by generating decoys in this manner. Accordingly, Applicants respectfully assert that claims 1 and 31, and claims depending therefrom, are patentable over the Schmidt reference (either alone or in combination with other references described herein).

(2) US Patent Application No. 2002/0082999, published on June 27, 2002, and filed by Lee (the "Lee reference").

The Lee reference describes a method of preventing a reduction of sales of records due to illegal distribution of music files through communication networks. In general, as described by Lee at pages 2-4 and in the accompanying figures, the Lee system includes the use of a service provider to produce an "advertising digital music file". In the example described in paragraph [0031], Lee describes a process where a digital music file is created in an MP3 format from a source record. The sound quality of the digital music file is then deteriorated or damaged. The digital music file is then distributed over a file sharing network as described in conjunction with Lee's FIG. 2.

The Lee reference does not teach or suggest a method such as claimed in Applicant's independent claims 1 and 31, where at least first and second reference files are created (in different formats) for each item of content to be protected. Nor does Lee describe a method where at least two sets of decoy files are created, each having defects, and each created from the different reference files. In this manner, embodiments of the present invention permit the creation and dissemination of a number of different types of decoys which mimic the type and format of files which are being copied on the file sharing networks.

Lee further fails to teach or suggest features of other claims of the present application. For example, Lee fails to teach or suggest the use of: dissemination agents to disseminate decoys (as claimed in claim 2, e.g.); query agents to submit various queries (as claimed in claim 3, e.g.); the registration of agents based on a network syntax and connectivity (claim 4); analyzing a file sharing network to identify an effect of decoy dissemination (claims 5-8); marking decoys to uniqely identify or validate them from other items of content (claims 21-22 and 28-29); introducing multiple or different defects in sets of decoy files (claim 24). Further, there is no teaching or suggestion in Lee to modify Lee to provide any of these features of embodiments of the present invention.

(3) U.S. Patent Application No. 2002/0087885, published on July 4, 2002, and filed by Peled et al. (the "Peled reference").

The Peled reference describes a method for monitoring a file sharing system and for applying a reactive defense against illegal distribution of content the file sharing system. As described in the Peled reference at page 4, the system includes a "surveillance element" which monitors networks to detect illegal or unauthorized distribution of content. If such unauthorized distribution is found, "offensive elements" may be used to attempt to interfere with the illegal or unauthorized activities. The "offensive elements" described by Peled include "internal offensive or attack elements" and "external offensive elements". Examples of these offensive elements include: "denial of service attacks" or saturation of a distributor of unauthorized content (e.g., see FIGs 5-8 and accompanying text); "intercepting requests for illegal content and replying to them by sending a version of the content that does not satisfy the user" (see FIG. 10 and accompanying text); malformed messages, etc.

The Peled reference fails to teach or suggest features of embodiments of the claimed invention. As with the Lee reference, Peled fails to teach or suggest a method where at least first and second reference files are created (in different formats) for each item of content to be protected. Nor does Peled describe a method where at least two sets of decoy files are created, each having defects, and each created from the different reference files. In this manner, embodiments of the present invention permit the creation and dissemination of a number of

different types of decoys which mimic the type and format of files which are being copied on the file sharing networks. As a result, the Peled reference (alone, or in combination with other references described herein) fails to teach or suggest embodiments of the present invention as set forth in independent claims 1 and 31. The dependent claims are believed patentable at least as depending from the patentable base claims.

(4) PCT Application No. WO 01/06373, published on January 25, 2001, filed by Lyle et al. (the "Lyle reference").

The Lyle reference describes a system and method for generating fictitious computer file system content (or, "honeypots"). In general, the fictitious computer file content generated by the system of the Lyle reference is generated by (or on behalf of) an entity operating a network The files are created using templates. As with the Lee, Peled and Schmidt references, the Lyle reference fails to teach or suggest a method as claimed in independent claims 1 and 31 of the present application where at least first and second reference files are created (in different formats) for each item of content to be protected. Nor does Lyle describe a method where at least two sets of decoy files are created, each having defects, and each created from the different reference files. In this manner, embodiments of the present invention permit the creation and dissemination of a number of different types of decoys which mimic the type and format of files which are being copied on the file sharing networks. The Lyle reference fails to teach a system for disseminating decoys to combat unauthorized copying as described in the instant application. Instead, Lyle describes techniques used to lure intruders into taking specific actions.

The Lyle reference fails to teach or suggest (alone or in combination with other references described herein) embodiments of the present invention as claimed in independent claims 1 and 31. The dependent claims are believed patentable at least as depending from the patentable base claims.

(5) "A Modified Depensation Model for Peer to Peer Networks: Systemic Catastropes and Other Potential Weaknesses", Chen et al

The Chen reference describes a modified version of a "depensation model" to describe potential susceptabilities of peer to peer networks to certain catastrophes. One of the catastrophes discussed is the use of fake users that carry incorrectly named or damaged files. No discussion of how the incorrectly named or damaged files are introduced, developed, or disseminated is provided. Instead, Chen focuses on identifying potential actions which could lead to degraded (or failed) network performance. The Chen reference fails to teach or suggest embodiments of the present invention as claimed in independent claims 1 and 31 at least because chen does not teach a method where at least first and second reference files are created (in different formats) for eachitem of content to be protected. Nor does Chen describe amethod where at least two sets of decoy files are created, each having defects, and each created from the different reference files. Other features of embodiments of the present invention (e.g., as claimed in dependent claims) are also lacking from the Chen reference.

Other Background Art

A number of references are cited which are considered as general background material, and may be grouped in three in three general categories: (1) background materials on network defenses; (2) background materials describing pirating of content on peer to peer networks; and (3) background materials describing the introduction of decoys in peer to peer networks. Several references uncovered by the search relate to network defenses (e.g., such as the honeypots and other deception techniques discussed in the two Recourse Technology white papers, or the distributed denial-of-service attacks described in the "Source Router Approach to DDOS Defense" article). Several references uncovered by the search relate to general discussions of the problem of pirating content on peer to peer networks. For example, the article "File Tracker May Go Too Far" describes software provided by MediaForce allowing the tracking of copyrighted content. The article "Box Office Hits Pirated Over the Web" discusses piracy of movies. A number of other cited references further describe the problem of content piracy.

Several references describe the introduction of damaged content or decoys in peer to peer networks. For example, the article "Music Industry Swamps Swap Networks With Phony Files" describes the general concept of placing bogus copies of popular songs on file sharing networks. The article (and other articles uncovered by the searcher) describe the general concept of placing bogus copies on networks. The references to not teach or suggest a method such as claimed in Applicant's independent claims 1 and 31 where at least first and second reference files are created (in different formats) for each item of content to be protected. Nor do the references describe a method where at least two sets of decoy files are created, each having defects, and each created from the different reference files. Accordingly, Applicants respectfully assert that the inventions as set forth in claims 1 and 31 are patentable over the references, alone or in combination. Dependent claims are patentable at least as depending on the patentable base claims.

Conclusion

It is respectfully submitted that the claims pending are patentable over the above-described art and the other references cited by Applicants. Expedited examination of the application, and issuance of a Notice of Allowance, are earnestly solicited.

Respectfully Submitted,

August 23, 2002
Date

Kurt M. Maschoff
Attorney for Applicants
Reg. No. 38,235